REMARKS

Claim 11 has been amended. Claims 29-49 have been added. Claims 1 – 49 are pending in the application. Applicants appreciate the indication of allowable subject matter.

REJECTIONS BASED ON THE CITED ART

Claims 11-15, 17-20, and 22-25 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,668,877 to Aziz, hereinafter Aziz.

Claims 16 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz in view of U.S. Patent No. 6,629,243 to Kleinman, et al., herinafter Kleinman.

The rejections are traversed for the reasons discussed below.

Claims 11-15, 17-20, and 22-25

Claim 11, as amended, recites "[a] method for establishing a secure communication session among a first node of a network and **two or more other nodes** that are joined in a first network communication entity ...." Specifically, Claim 11 recites among other things:

> communicating a first public key value from a first node that is joining the first network communication entity to each other node that is currently within the first network communication entity;
>
> computing a new group shared secret key based on the collective public key value and the private key value associated with the first node;

where the "collective public key value is shared by each other node in the first network communication entity," the first network communication entity comprises of "two or more other nodes," and the "first node" is "joining the first network communication entity." Furthermore, in

order for a secret key to be analogous to the "group shared secret key" of Claim 11, that secret key must be **computed based on** both (a) a collective public key value of the group and (b) a private key value of the node that is joining the group.

As is discussed in Applicant's previous response, neither K_g nor K_p of Aziz in multicast situations possesses these characteristics. Furthermore, neither K_{ij} nor K_p of Aziz in two-node situations possesses these characteristics. Aziz does not appear to disclose any group shared secret key that is created based on both (a) a collective public key value of the group and (b) a private key value of the node that is joining the group.

The Office Action cites Aziz, col. 2, lines 20-44, col. 4, lines 33-53, and col. 8, line 30 to col. 9, line 67 as meeting the "computing" features of Claim 11. However, the passage in Aziz, col. 2, lines 20-44 does not disclose a collective public key value of a first network community entity of two or more nodes. First, K_{ij} of Aziz is not communicated, but calculated by each node I or J (col. 2, line 29). Second, K_p of Aziz is only a transient, thrown-away key whose value changes after a certain number of bytes have been exchanged by two nodes already forming a group (col. 2, 32-35), and not used to form the group in the first place. Third, only two nodes are involved with respect to either K_{ij} or K_p in this cited passage, as opposed to Claim 11 where a new node joins an entity which already comprises two or more nodes. Clearly, neither K_{ij} nor K_p is a collective public key whose existing value is communicated and re-computed at the time when a new node joins to form a new network community, as disclosed by Claim 11.

Similarly, nowhere in Aziz, col. 4, lines 33-53 discloses computing a collective public key value by both a new node and two or more nodes in a first network community entity. The passage only talks about communicating a group interchange key, G_p, to a requesting node.

Lastly, the passage in Aziz, col. 8, line 30 to col. 9, line 67 talks about how the value of K_{ij} can be changed by two nodes already forming a group. This passage has nothing to do with joining of a new node to a network community entity. Rather, it talks about how two nodes already forming a group can implicitly calculate a new value of K_{ij} based on SAID field in IP packets exchanged (SAID (N) in Fig. 6).

Since none of the cited passages in Aziz discloses a feature of calculating a new collective public key value for the purpose of joining a new node to a network community entity, Claim 11 recites features that Aziz does not disclose. Consequently, Claim 11 is patentable over Aziz under 35 U.S.C. §102(b).

Claim 20 recites "**computing** a new shared secret key by the new node **based upon** the common public key of the multicast group and the new private value;" where the "new private value" is generated by a "new node" that joins the multicast group. Thus, the "new shared secret key" of Claim 20 must be computed based upon both (a) "the common public key of the multicast group" and (b) a new private value generated by a new node that joins the multicast group.

As is discussed above with regard to Claim 11, Aziz does not disclose any shared secret key that is computed based specifically upon such keys and values. Consequently, Claim 20 is patentable over Aziz under 35 U.S.C. §102(b).

Claims 12-15, 17-19, and 22-25 comprise the distinguishing features of Claim 11 or 20 by virtue of their dependence from Claim 11 or 20. Therefore, Claims 12-15, 17-19, and 22-25 are likewise patentable over Aziz under 35 U.S.C. §102(b).

Claims 16 and 21

Claims 16 and 21 depend from independent claims discussed above. By virtue of this dependence, Claims 16 and 21 comprise the features of the claims from which they depend—features that are distinguished from Aziz above.

The Office Action does not rely on Kadansky to disclose these distinguishing features. The Office Action only relies on Kadansky to disclose, allegedly, the step of storing and distributing public values using a key distribution center. Since neither Aziz nor Kadansky discloses the distinguishing features discussed above, even the combination of Kadansky with Aziz lacks the distinguishing features of Claims 16 and 21.

Therefore, Claims 16 and 21 are patentable over the combination of Aziz and Kadansky under 35 U.S.C. §103(a).

CONCLUSION

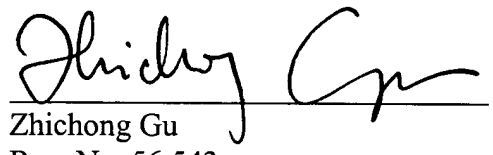
For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to deduct any applicable fees from and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: April 25, 2006



Zhichong Gu
Reg. No. 56,543

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076